The Powers of Fault Tree Analysis

Bill Vesely

Office of Safety and Mission Assurance

NASA Headquarters

Fault Tree Analysis: a Systematic and Stylized Deductive Process

- An *undesired event* is defined
- The event is resolved into its *immediate causes*
- This resolution of events continues until *basic causes* are identified
- A logical diagram called a *fault tree* is constructed in the process of carrying out the analysis

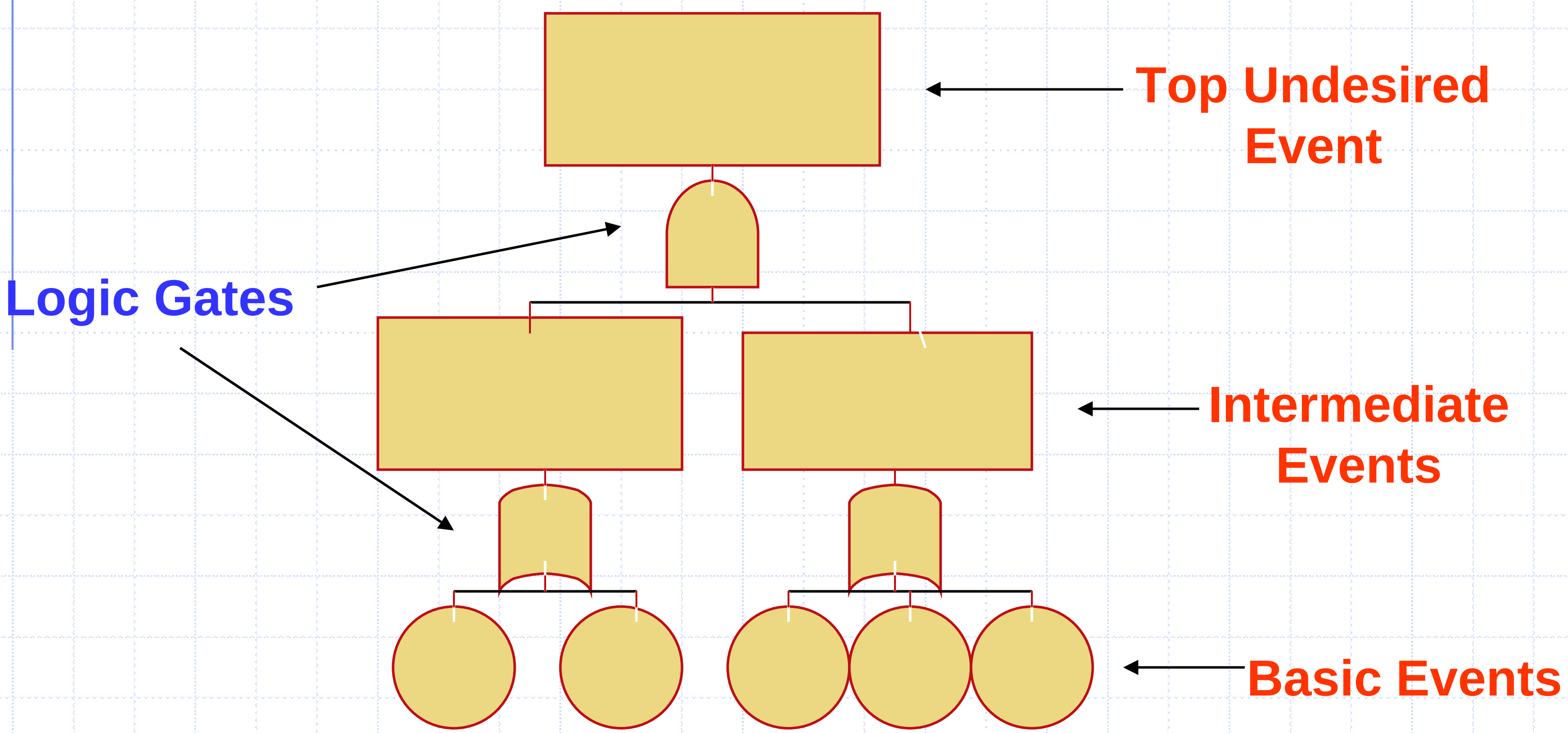
Why Fault Tree Analysis (FTA) is carried out

- To gain an understanding of the system
- To document the failure relationships of the system
- To exhaustively identify the causes of a failure
- To assure compliance with requirements or a goal
- To identify any weaknesses in a system
- To prioritize contributors to failure
- To identify effective upgrades to a system
- To optimize operations and processing
- To quantify the failure probability and contributors

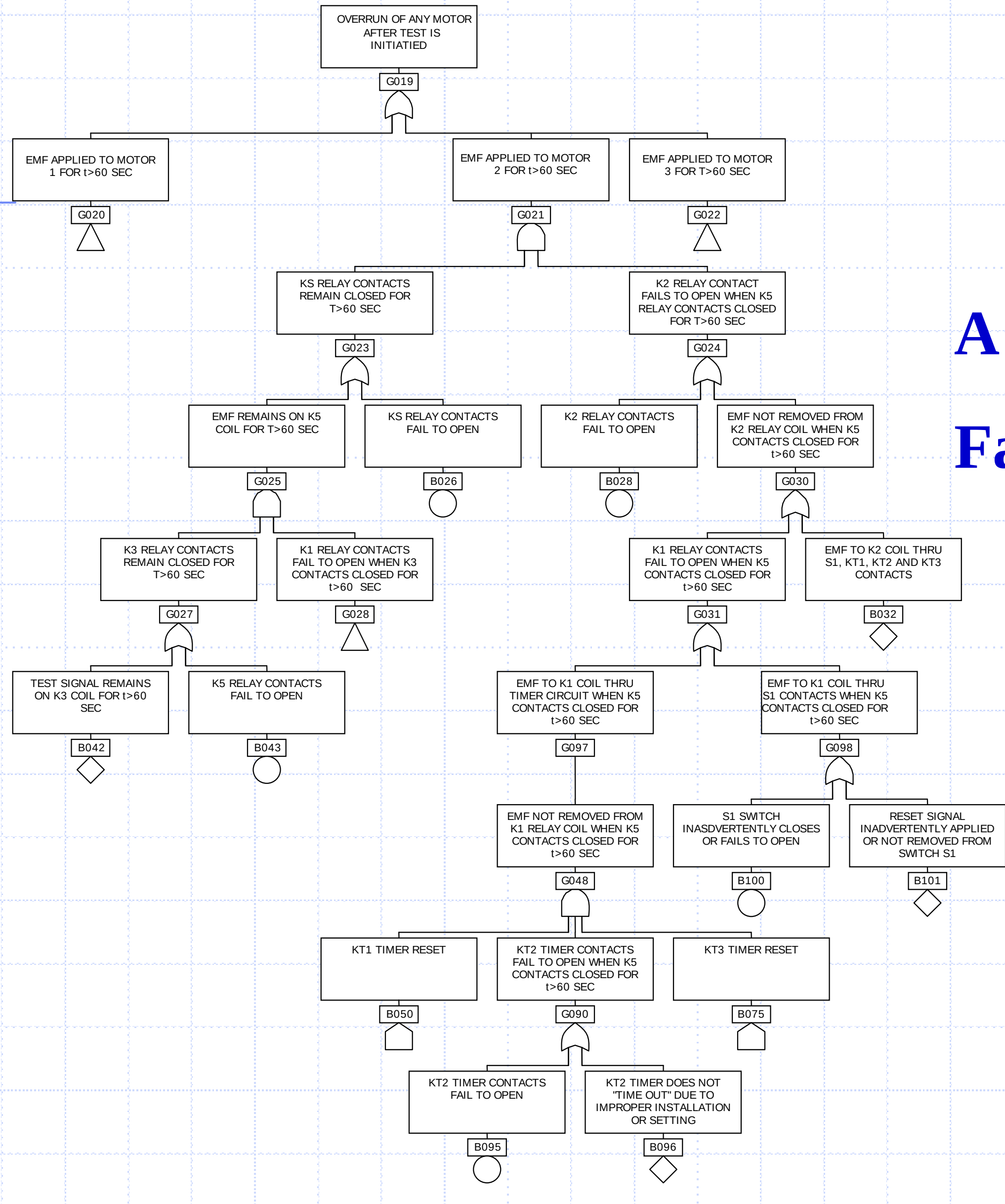
The Fault Tree

- FTA produces a *Fault Tree.*
- The fault tree is the *logical model* of the relationship of the undesired event to more basic events.
- The *top event* of the fault tree is the undesired event.
- The *middle events* are intermediate events.
- The bottom of the fault tree is the causal *basic events* or *primary events*.
- The logical relationships of the events are shown by logical symbols or *gates*.

Basic Fault Tree Structure



A Typical Fault Tree



Applications of FTA

- Identification of the Causal Contributors
- Prioritization of Contributors for Resource Allocation
- Development of a Design
- Determination of Effective Tradeoffs
- Resolution of Causes for Mishap Analysis
- Demonstration of Compliance with Single Failure Criteria
- Establishment of Contingency Criteria
- Monitoring and Tracking of Performance

Identification of the Causal Contributors

- FTA identifies the minimal cut sets of the undesired top event
- A minimal cut set is a smallest combination of basic causal events that results is the occurrence of the top event
- The set of minimal cut sets gives all the possible combinations of basic causal events that cause the top event
- The minimal cut sets are thus the “basic causes” of the top event

The Minimal Cutsets Provide Key Qualitative Information

- The minimal cutsets directly link the top event to the primary events, or basic events
- The minimal cutset (mcs) *size* is a qualitative ranking of the causal-combination
- A *single element* mcs identifies a single cause of the top event
- The component *types* in the mcs also provides a qualitative ranking of the causal combination
- *Redundant components in a* mcs can be susceptible to a common triggering cause

Example of Minimal Cutsets for a Monopropellant System Fault Tree

Primary Time out Failure of K6 • Operational Failure to Open of S3
Primary Time out Failure of K6 • Primary Failure to Open of S3
Primary Failure to Open of K6 • Operational Failure to Open of S3
Primary Failure to Open of K6 • Primary Failure to Open of S3
Primary Failure to Close of IV2 • Primary Failure to Open of K5
Primary Failure to Close of IV2 • Primary Failure to Open of K3
Primary Failure to Close of IV2 • Primary Failure to Close of IV3

The Power of FTA in Prioritizing Failure Contributors

- Each basic event in the fault tree can be prioritized for its importance to the top event
- Different importance measures are obtained for different applications
- Basic events generally are ordered by orders of magnitude in their importance.
- In addition to each basic event, every intermediate event in the FT can be prioritized for its importance
- As a general rule, less than 20% of the contributors result in more than 90% of the risk.

Basic Fault Tree Importance Measures

FV Importance = Relative contribution to the system failure probability from a component failure

RAW = Factor increase in the system failure probability when a component is assumed to be failed

RRW = Factor decrease in the system failure probability when a component is assumed to succeed

FV Importance = "Fussell-Vesely Importance"

RAW = "Risk Achievement Worth"

RRW = "Risk Reduction Worth"

Basic Causal Importances for a Monopropellant System

Basic Causal Event	FV Importance (Contribution)	RRW Factor (Reduction)	RAW Factor (Increase)
Human Error Failure to Open Switch S3	99.3%	143	100
Timer K6 Fail to Time Out	86.7%	7.5	43
Relay K6 Fail to Open	13%	1.15	43
Switch S3 Fail to Open	0.5%	1.01	100
Isolation Valve IV2 Fail to Close	0.3%	1.00	13
Relay K3 Fail to Open	0.3%	1.00	1.00
Isolation Valve IV3 Fail to Close	0.01%	1.00	1.00

Uses of the Importance Measures

- Focus system safety on the top contributors (FV)
- Review possible relaxations for the lowest contributors (FV, RAW)
- Focus on upgrades having the greatest improvements (RRW)
- Define contingency measures to be consistent with the failure impact (RAW)
- Establish assurance requirements to be consistent with their importance (FV, RAW)

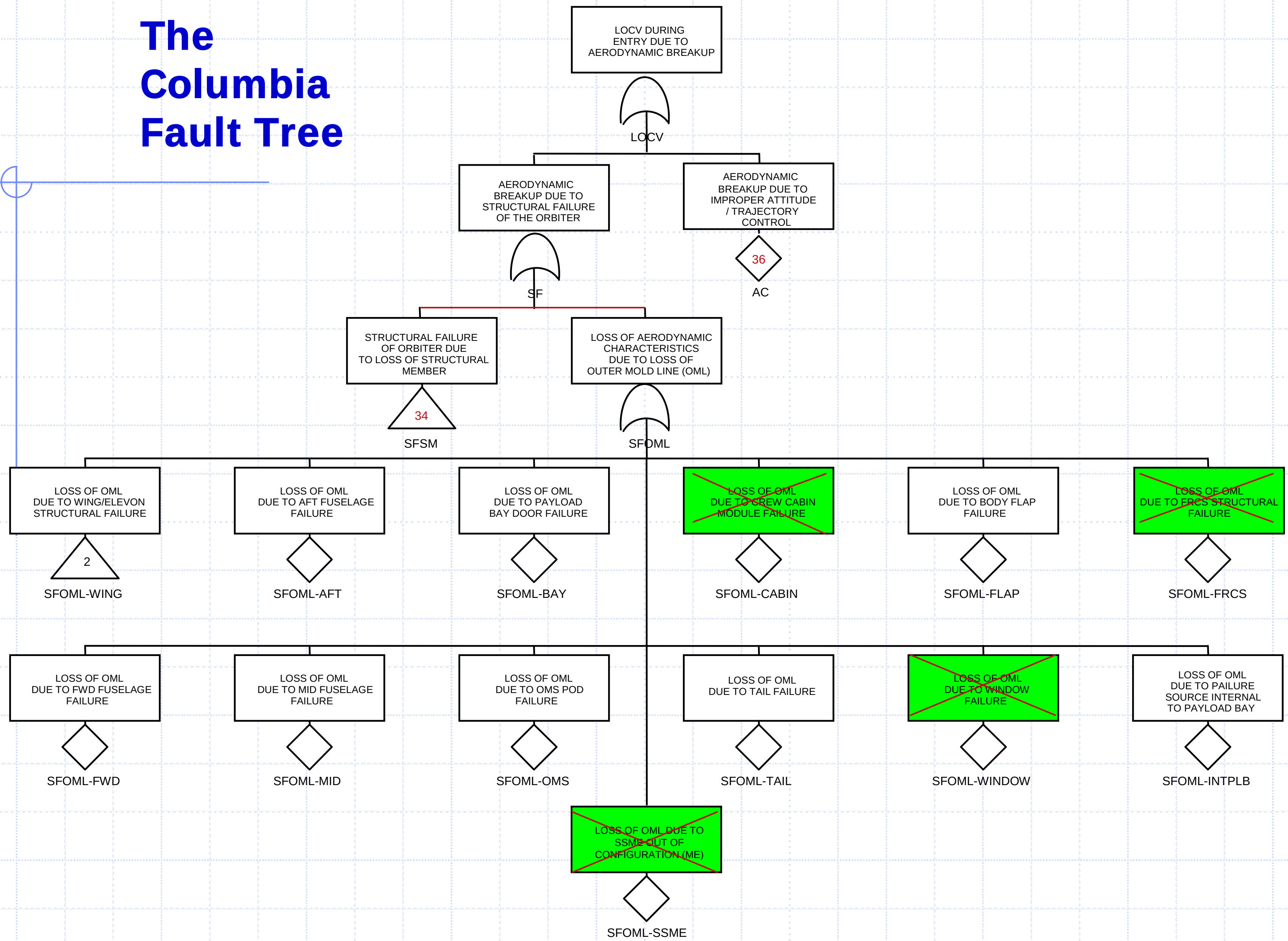
Examples of Importance Evaluations in the Space Shuttle PRA

- Over a million individual events are modeled in the Shuttle PRA and 97% of the calculated risk resides in approximately 308 events.
- Approximately 15% or more of the calculated risk is due to fluid leaks that lead to fire and explosion. This can change based on current updating of the Shuttle PRA
- Abort risk is insignificant to mission risk (<1%).

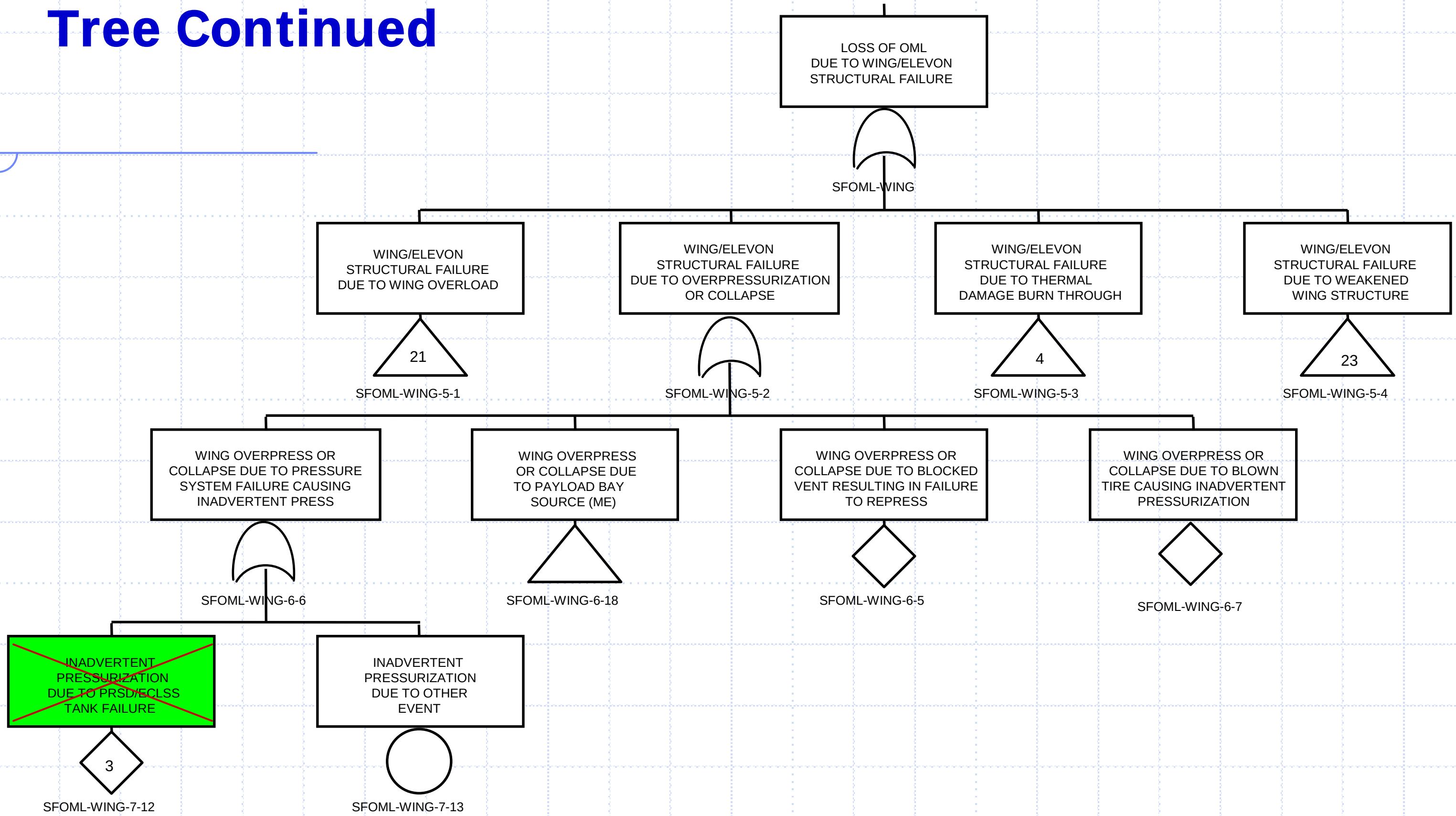
The Use of FTA in Mishap Analysis

- The accident scenario is constructed for the mishap
- System failures (pivotal events) are identified which resulted in the mishap
- A fault tree is constructed for each system failure to resolve the basic events involved
- Root cause analysis is carried out by further resolving a basic event into its root causes
- The basic events and root causes are dispositioned into their importances and actions required

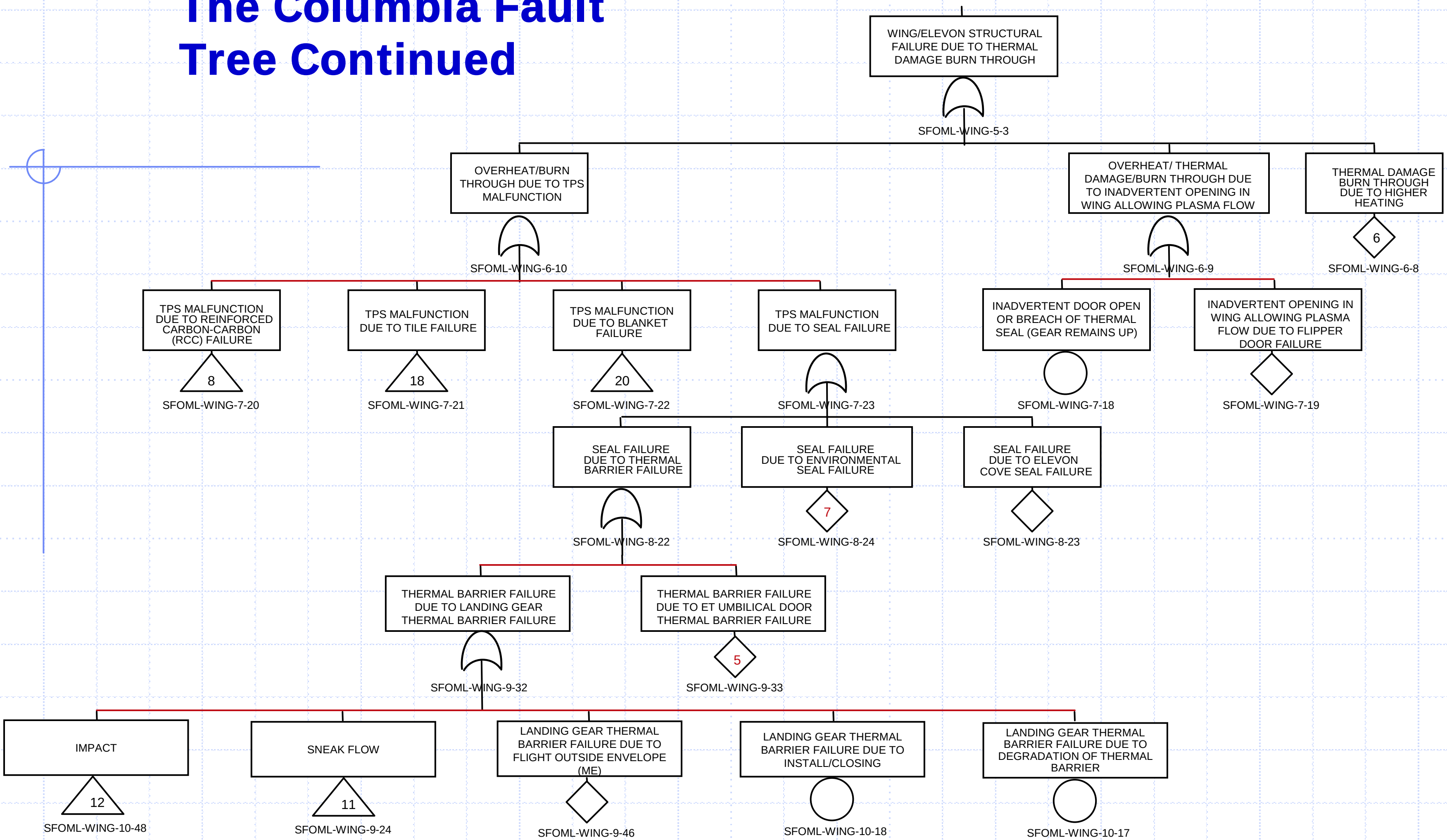
The Columbia Fault Tree



The Columbia Fault Tree Continued

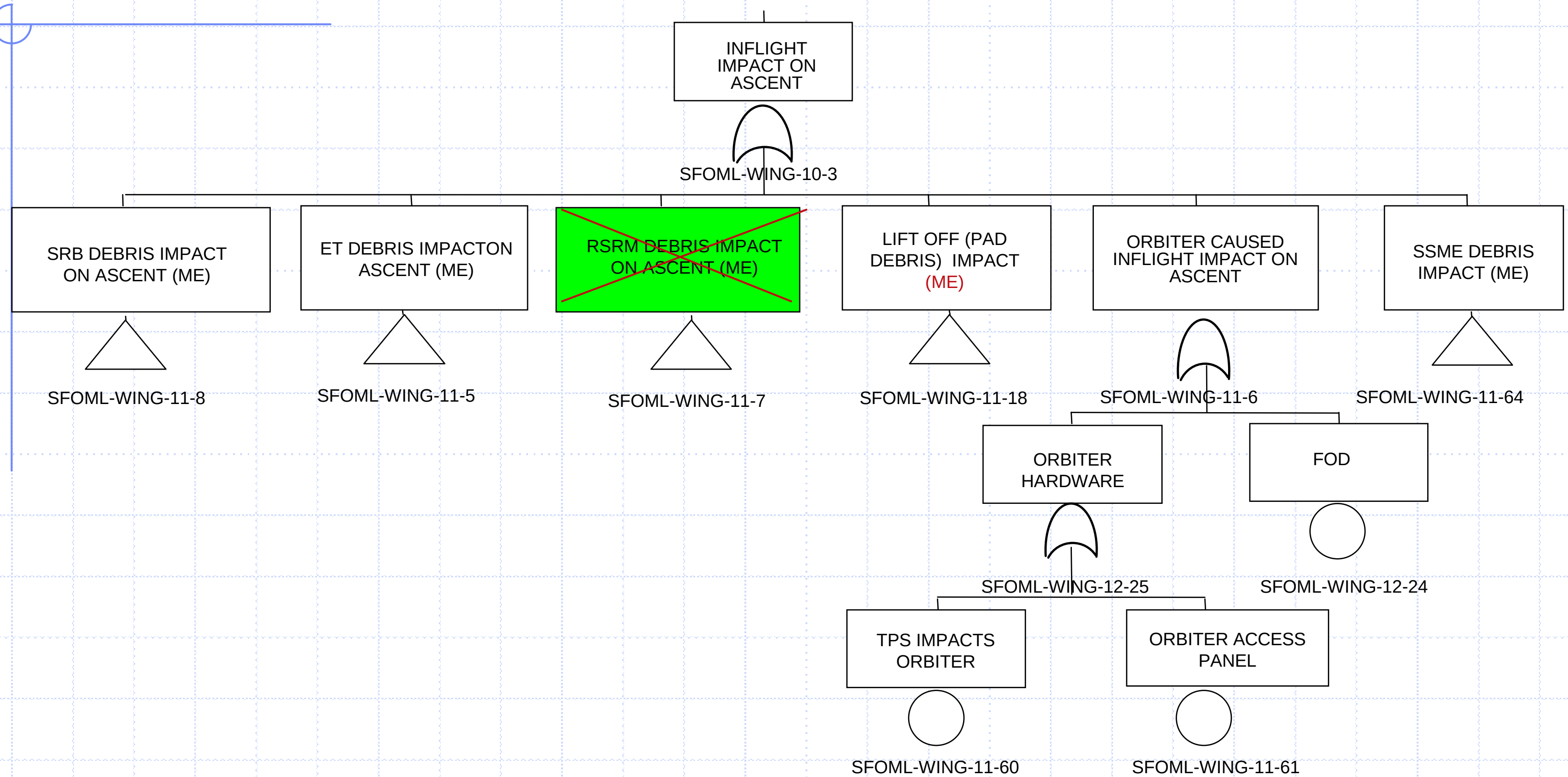


The Columbia Fault Tree Continued



SFOML-WING-5-3 - WING/ELEVON STRUCTURAL FAILURE DUE TO THERMAL DAMAGE BURN THROUGH 2003/04/18 Page 4

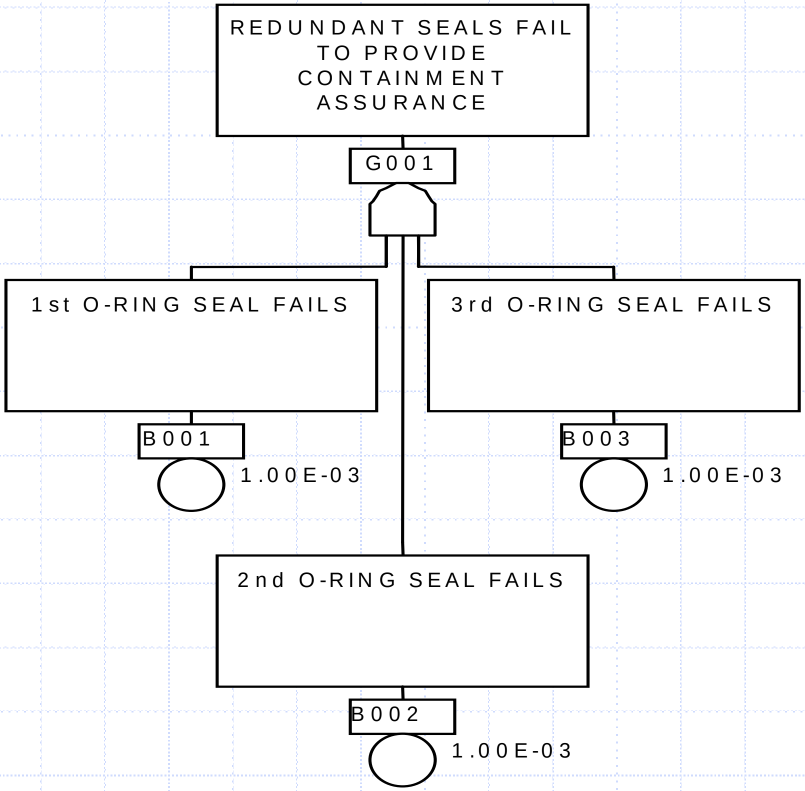
The Columbia Fault Tree Continued



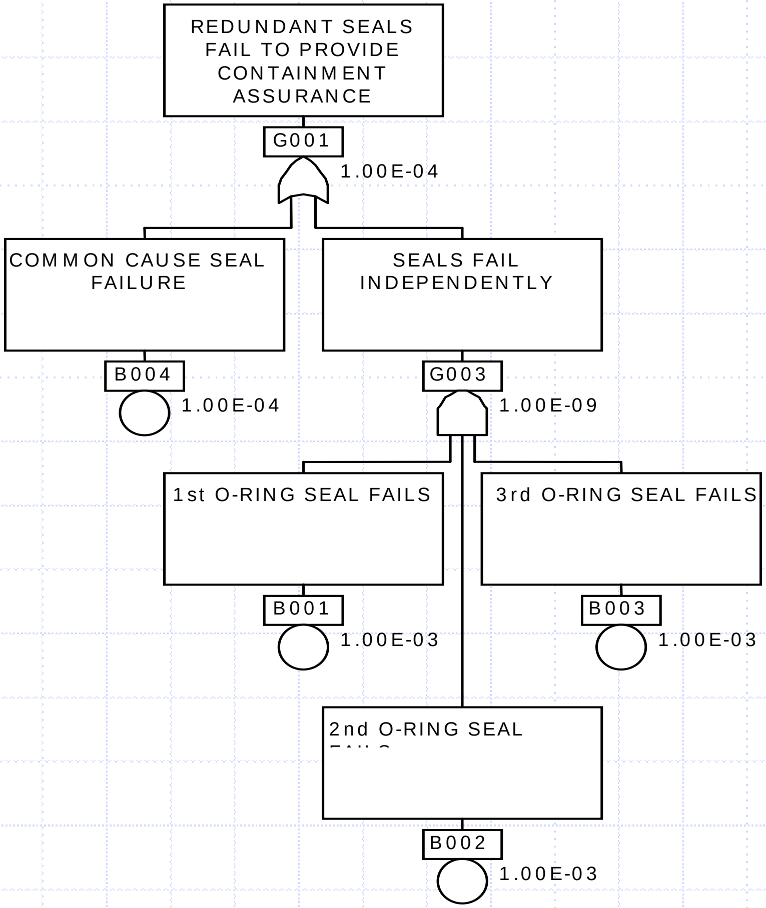
The Use of FTA in Design

- To evaluate a Design, a top level fault tree is developed
  - Functional level
  - System level
  - Subsystem level
- Tradeoffs are carried out
  - Alternative functional capabilities
  - Alternative redundancies
- Allocations are performed
  - System requirement into subsystem requirements
  - Subsystem requirements into component requirements

Redundant Seal Design Allocation Considering Independent Failures



Redundant Seal Design Allocation Including Common Cause Failures



The Fault Tree as a Master Logic Diagram

- The Master Logic Diagram (MLD) is a fault tree identifying all the hazards affecting a system or mission
- The Master Logic Diagram can also be called a Master Hazards Diagram (MHD)
- The MLD or MHD is developed using fault tree logic
- The basic events of a system MHD are the hazards that can initiate component failures or increase their likelihood
- The basic events of a mission MLD are the hazards that are the initiating events of potential accident scenarios

Extending a System Fault Tree to a Master Hazard Diagram (MHD)

- The top event is defined as a system failure event
- The fault tree is developed to the basic component level
- Each component failure is further resolved into hazards and conditions that can cause failure or increase its likelihood
- The resulting system MHD identifies the hazards affecting the system and their consequences
- Of particular importance are single failures and hazards affecting multiple redundant components

Ranking the Criticality of Hazards Using FTA

- Each hazard is linked to a basic event or events on the fault tree
- Equivalently each hazard is linked to the basic events in the minimal cutsets
- The criticality of the hazard is the likelihood of the hazard times the importance of the basic event
- The component importance is determined from the FTA
- The likelihood is determined from the hazard analysis

Hazard Criticality=Likelihood x Importance of Components Affected

Mission

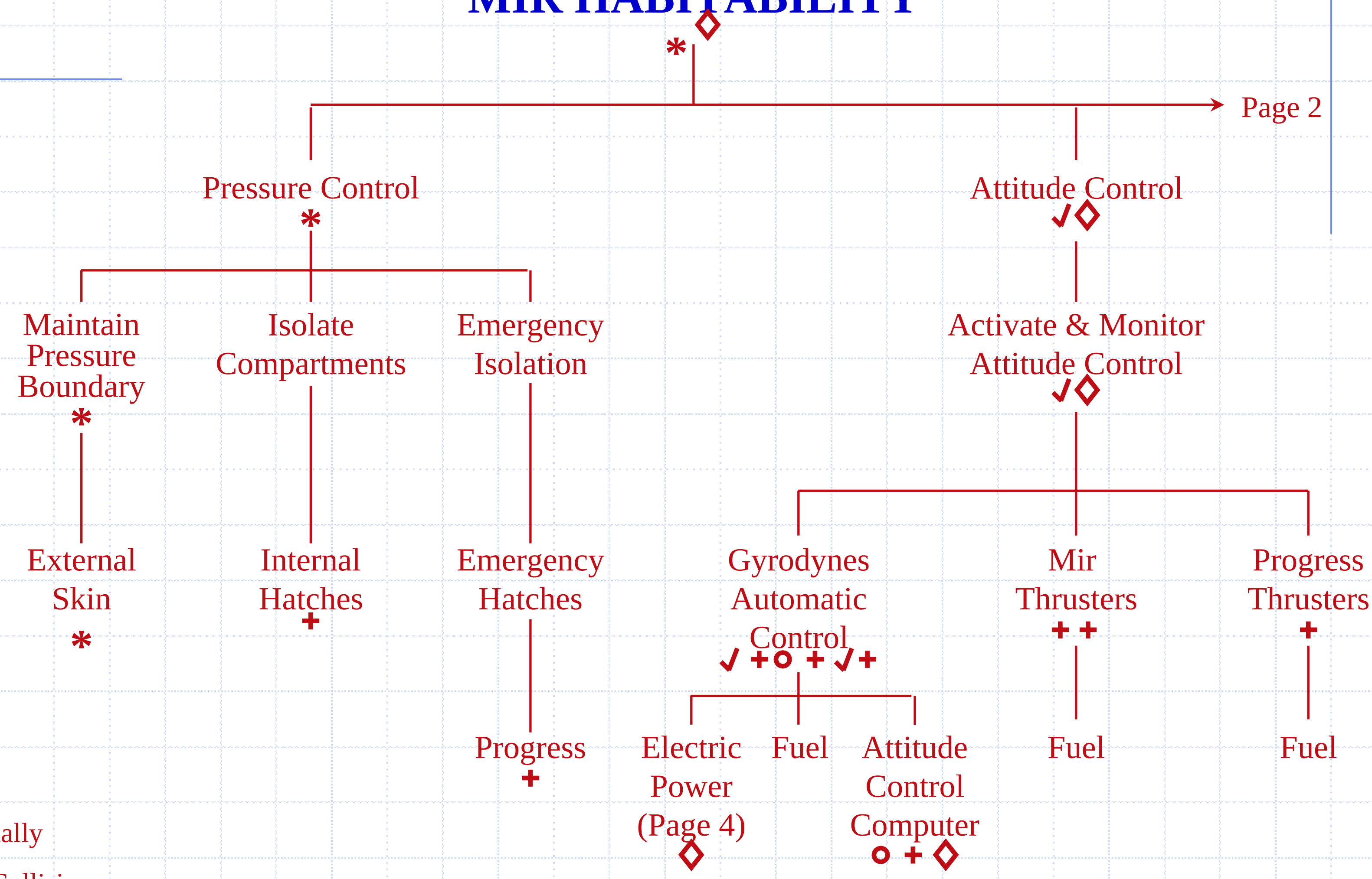
Critical Functions

Tasks

Resources

Support Systems

MIR HABITABILITY



+ Activated Manually

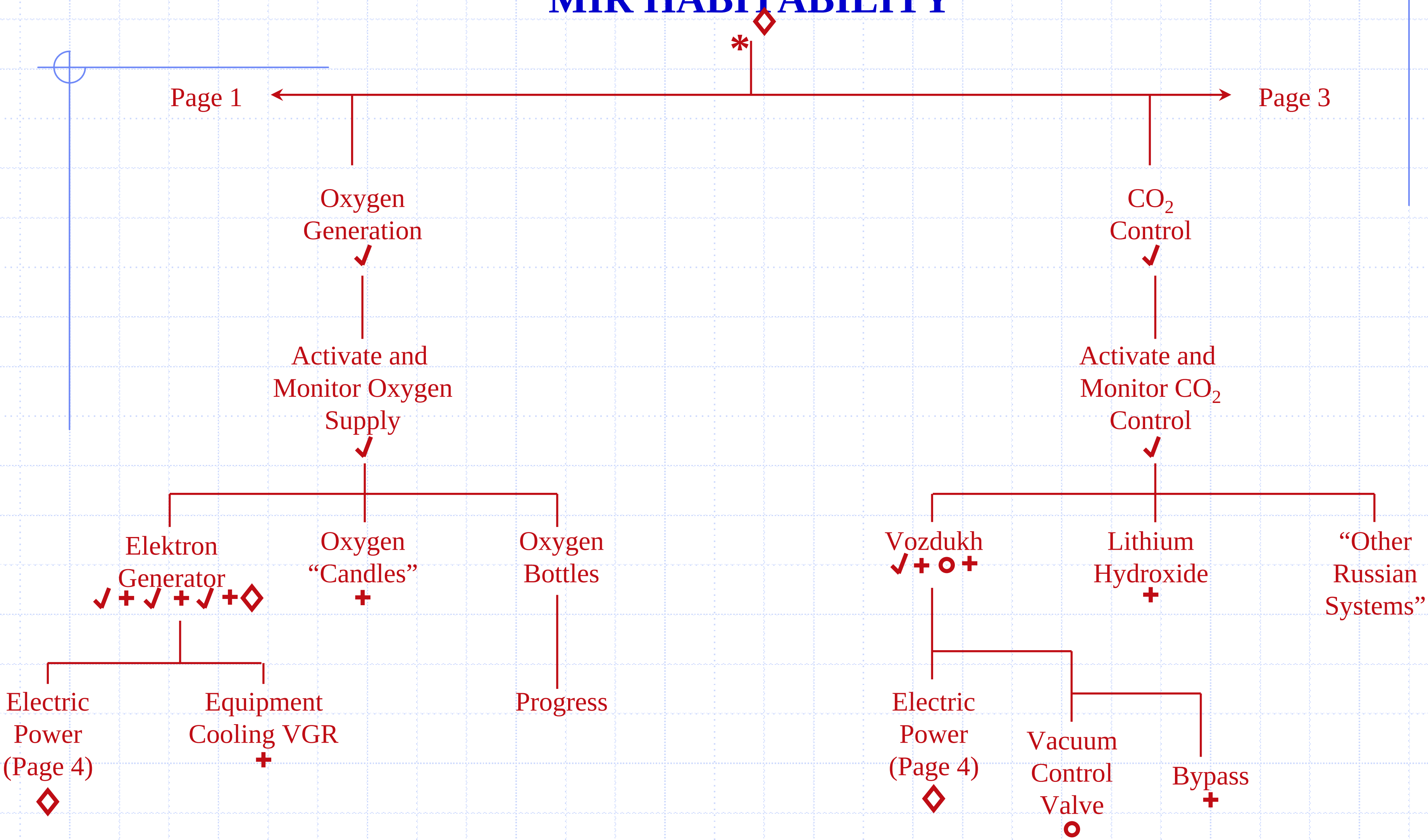
* Challenged by Collision

✓ Challenged by Manual Action

o Equipment Failure

◇ Disabled/Challenged by Human Error

MIR HABITABILITY



The Mirror Success Tree (ST)

- A Success Tree (ST) identifies all the ways in which the top event *cannot* occur
- The ST is the *complement* of the FT
- The ST is the *mirror* of the FT
- The ST is useful in showing the explicit ways to *prevent* the occurrence of the FT
- The ST is the *success space* twin of the FT

Developing the Success Tree from the Fault Tree

- Complement the top event to a NOT event
- Complement all intermediate events to NOT events
- Complement all basic events to NOT events
- Change all AND gates to OR gates
- Change all OR gates to AND gates
- The tree is now the ST
- The minimal cut sets of the ST are now called the minimal path sets

The Minimal Path Sets Define the Success Modes of the System

- A minimal path set is the smallest number of events which if they all do not occur then the top event will not occur
- If the events in one path set are prevented to occur then the top event will be guaranteed to not occur
- The minimal path sets are the totality of ways to *prevent* the top event based on the fault tree
- The minimal paths should be determined as a part of a fault tree analysis

FTA Project Management Tasks (1)

- Define the FTA
  - Top Event
  - Scope
  - Resolution
- Assemble the project Team
  - FT analyst
  - System engineering support
  - Data support
  - Software support
- Define the FTA Operational Framework
  - Assemble the as built drawings
  - FT naming scheme
  - Interfaces/Support to be modeled
  - Software to be used

FTA Project Management Tasks (2)

- Assemble the data
  - Generically applicable data
  - Specifically applicable data
- Prepare the software package
  - Familiarization
  - Test problems
- Keep a log on the FTA work
  - Operational and design assumptions
  - Events not modeled and why
  - Success and failure definitions
  - Special models and quantifications used

FTA Project Management Tasks (3)

- Review the work at stages
  - FT construction
  - Qualitative evaluations
  - Quantitative evaluations
- Check and validate the results
  - Engineering logic checks
  - Consistency checks with experience
- Prepare and disseminate the draft report
  - Conclusions/findings
  - FTA results
  - FTs
  - Software inputs/outputs
- Obtain feedback and modify and final report
  - Disseminate the report
  - Present findings

Reference

- “Fault Tree Handbook with Aerospace Applications’, Version 1.1, NASA Publication, August 2002.